PATENT APPLICATION IN FRANCE

FILED ON 28 APRIL 2000

UNDER NATIONAL REGISTRATION NO. 00/05,517

IN THE NAME OF : **AIRSYS ATM S.A.**

WITH THE TITLE : **REDUNDANT INPUT / OUTPUT MANAGEMENT DEVICE, NOTABLY FOR COMPUTERIZED ROUTING**

INVENTOR : **Laurent BARETZKI**

THOMSON GROUP (TPI/DB) REFERENCES :
(X 7712 - AIRSYS ATM)

DRAWN UP AT THE TPI/DB BY : M. LAURENT LUCAS

PATENT DEPARTMENT (TPI/DB) OF THE THOMSON GROUP
ADDRESS: 13, AVENUE DU PRESIDENT SALVADOR ALLENDE - 94117 ARCUEIL CEDEX

The present invention relates to a redundant input/output management device, notably a computerized routing system. It applies in particular in respect of the processing of air traffic management information. More generally, it applies in respect of all digital data input and output management systems requiring high security of operation without excessive cost overheads.

Air traffic density has reached a very significant level. Additionally, air safety requirements are still ever growing. A consequence of this situation is that air traffic management has to process a large amount of information, intended notably for air traffic controllers and aircraft pilots. This information pertains in particular to a wide category of radar data, meteorological situations, flight plans or else data of ILS type relating to landing systems.

The processing of this information can only be handled by powerful computing means. Among these means, an essential role is played by the interfacing means of the various information or decision centres. These interfacing means have notably an information routing function, they therefore have notably a function of steering the data to the proper destination centres. Given the very significant data flows involved, these means have an essential role in respect of the proper overall operation of an air traffic management system. The processed data are notably radar data and other data relating to the flight situation of aircraft, such as for example flight plans or meteorological information.

There exists known hardware, notably available commercially, equipped with its operating systems, which makes it possible to meet these routing requirements. By way of example, mention may be made of a range of products known by the trademark LINES

arising from the expression "Link Interface Node for External Systems". These products, of modular type, are designed to allow the routing and processing of input/output messages from among incoming or outgoing serial and Ethernet lines. Standard serial lines such as for example X25, HDLC or BSC are processed in addition to dedicated lines, such as for example particular radar information transmission protocols.

These routers can operate with a software architecture of front-end processor type. They are equipped with software of FPBSS type, the latter term arising from the expression "Front Processor Basic System Software". In this embodiment, the router is linked to a single application program. It has only an upstream function, for example the steering of the data to the proper destination. The whole of the core of the application package is in one or more central computers. Stated otherwise, as many routers as application packages are necessary.

A more efficacious use of these routers can be achieved according to an open communication mode, also termed OCP, standing for the expression "Open Communication Processor". In this mode, a router is linked to several applications and operates substantially as a data server. It makes it possible notably to steer and to process the data from any input point to any output point. This mode of operation is particularly well suited to air traffic management. In an air traffic control management application, this mode in fact allows notably the following functionalities, that is to say:

- black-box type distribution of the radar data to the centres, the radar data being received through serial interfaces and transmitted via a local network, for example Ethernet, to a group of identified machines, broadcasting also called UDP

multicast in the literature;

- autonomous conversion of messages or protocols, allowing notably message format conversion or specific protocols, thus for example ISR2 into ASTERIX, X25 into HDLC-UI etc.;
- a line monitoring function in radar systems, that is to say the transmission of radar data through serial lines to the processing circuits.

In an application of air traffic management type, the security of operation of the computer systems, and therefore of the routing systems, is of prime importance, since the safety of the passengers is in fact involved. By way of example, the safety standards in force require that the aerial coverage of an air traffic control centre must not be interrupted for more than a few seconds a year. It is therefore necessary to resort to redundancy techniques, that is to say in particular duplicating the equipment items so that one of them can substitute itself for the other in the event of a fault. As a general rule, each router is duplicated. A problem to be solved is the switchover from one router to another, when the first is faulty. A known solution consists in making provision for an active router, called the master, and an inactive router, called the slave, with a third party system which arbitrates the switchover of execution from the master to the slave. This solution is not economic by reason notably of the use of a third-party system, which is added to the redundant router.

To render the system economic, it is possible to dispense with the arbitrator. A protocol for exchanges between the master and the slave is then provided. In particular, when the master becomes faulty, the slave no longer receives any messages. The slave then takes over. However, there are degraded modes, notably where the master degrades the processed data without being

aware of it. The master not being aware that it is faulty does not deactivate its inputs/outputs. The slave on its side is aware that the master is faulty but is then not able to take control of the routing correctly, on account notably of the fact that the master has not deactivated its input/output ports. The system continues to operate in degraded mode. This results in a worrying degradation of the security of operation.

An aim of the invention is to reduce the costs related to security of operation, by dispensing with the use of a third-party arbitration system, doing so without degrading the security of operation whatever the types of input/output ports. For this purpose, the subject of the invention is a device for digital data input and output management, characterized in that it comprises first management means and second management means connected together by two interfaces, a network and a security line, these means mutually exchanging interrogation messages through these two interfaces, means being considered to be faulty by the other means when they do not send any message in a given time interval on at least one of the two interfaces.

The input and output management means can be routers or data servers.

On startup, the first means have for example the role of master and the second means the role of slave, the master managing the input and output data. To ensure redundancy, the means have the same functions and comprise the same software and same configuration files.

When means are detected as being faulty by the other means, the latter deactivate for example the faulty means. The slave can then take charge of the data management in place of the master.

Advantageously, the interrogation messages, the frequency at which these messages are dispatched, the limit time between two messages are installed in a configuration file contained in each of the means, several types of these parameters being stored depending on given applications. Thus, the parameters specific to an application can be offloaded to a random access memory during initialization of the device.

The main advantages of the invention are notably that it accommodates numerous applications and that it is simple to implement.

Other characteristics and advantages of the invention will be apparent with the aid of the description which follows offered in relation to appended drawings which represent:

Figure 1, an exemplary redundant routing system in the case where the input and output ports are of the serial type;

Figure 2, an exemplary redundant routing comprising a communication network, of the Ethernet type, with client stations.

Figure 1 presents an exemplary redundant routing system in the case where the input/output ports are of the serial type. The system comprises a router 1 having the function of master and a router 2 having the function of slave. These two routers have the same functions and comprise notably the same software and same configuration files. One and the same port 3 of each router communicates through a serial link with one and the same system 4, for example a modem. For this purpose, the link between the latter and the two routers is effected through a y-cable 5. A safety bus 6 links the two routers 1, 2.

When the two routers 1, 2 start up together, the master 1 activates its electrical modes on its input/output ports 3 while the slave 2 leaves its ports 3 inactivated, that is to say in the high-impedance state. This signifies that even if both routers are configured, only the master 1 exchanges with the modem 4. In the event of a fault with the master, two cases can notably occur:

- the master resets to zero or "resets" by placing its ports 3 in the high-impedance state and itself becomes slave, at the same time, the slave 2 becomes master and its ports are electrically activated, this is the normal situation which is simple to manage;
- the master becomes faulty, but does not "reset", the slave is aware that it ought to become master, but the current master does not deactivate its ports, there is therefore no switching from one router to another because of a potential conflict between the ports 3 of the two routers, this is the most complex situation to manage.

The second situation must however be dealt with since it dangerously affects security of operation. In this operating mode, the master may in fact process or route false data. To handle this problem, provision is made notably for the safety bus 6 connected between the two routers and intended to send it a "reset" command, that is to say a command for deactivating its ports 3, this command being sent by the slave. The latter can then retake control.

The type of redundancy architecture illustrated by Figure 1 is well adapted when the input/output ports involved are serial ports. This is no longer so when the router exchanges through a local network, called a LAN standing for the expression "Local Area Network", for example Ethernet.

Figure 2 illustrates an exemplary embodiment of a device according to the invention. It involves a computerized routing system comprising two routers 1, 2, one of which is master and the other slave. These two routers operate in OCP open mode. The device being made redundant, the two routers then comprise the same functions, and notably the same software and same configuration files. Likewise, the inputs and outputs to other systems are made redundant.

The two routers are for example linked by a network 23, for example Ethernet or Internet, to one or more remote client systems 21, 22. They are additionally linked to other systems, for example modems, by serial links. A y-cable 5 links one and the same port 3 of each router to one and the same system, in such a way notably that these two ports 3 can exchange with this system. When the master is active, its serial port is activated while that of the slave is inactivated, by being for example in the high-impedance state.

The two routers are linked together by the network 23, for example Ethernet or Internet, and by a security line 24, for example a bus. By way of example, an Ethernet network 23 is considered. On startup, or on initialization of the device, one router 1 is master and the other 2 is slave. It is the master which then manages the input and output data, therefore which routes them. During operation, the two routers 1, 2 mutually exchange interrogation messages, also called "polling messages" in the literature. These interrogation messages are for example exchanged cyclically, that is to say at regular time intervals. They are exchanged by the Ethernet network 23, for example by a broadcast of the UDP unicast type. Interrogation messages are exchanged also by the safety link 24. A device according to the invention therefore

comprises at least two interfaces for exchanging interrogation messages, a network interface, for example Ethernet, and a communication bus 24. An interrogation message is dispatched by the slave to the master to verify that the master is in a proper state to operate, to verify that it is not faulty. For this purpose, the master must respond to this message. All types of interrogation messages can be used. The simplest is for example to send the master a given message and verify that the latter returns it whole. On its side, the master sends from its side interrogation messages to the slave to verify that the latter is also in a state to operate. Therefore there is thus supervision of the two items of hardware 1, 2 without the aid of an equipment third party.

When the slave 2 does not receive at least one interrogation message in a given time interval on at least one of the two interfaces, Ethernet 23 or the safety link 24, its program considers that the master is faulty. The slave then decides to become master. For this purpose, it activates the switching mechanism. This switching mechanism can have several components. It comprises an algorithm, installed for example at one and the same time in the master and the slave, which forces the master to reset itself to zero, more particularly to reinitialize itself. This algorithm is programmed additionally so that during this reinitialization, the slave takes control, therefore becomes active in the processing of the data, while the master remains inactive. This algorithm additionally envisages the deactivation of the input/ouput ports of the master and the activation of the input/ouput ports of the slave that has become master. A supervision station 25 makes it possible for example to read fault or failure reports dispatched by the master or the slave. This station 25 can additionally be used for other functions within the general framework of the

application. The device comprises for example alert means for forewarning of a fault, so that the faulty hardware is replaced in due time.

The algorithm which forces the resetting to zero of the master, and ultimately its deactivation, is installed in the master, but it is activated by the slave. For this purpose, the slave knows the memory address of this algorithm. Preferably and in a symmetric manner, the algorithm is also installed in the slave, for hardware production standardization reasons, but also so that the master can completely deactivate the slave in the event of a fault with the latter. The reset to zero algorithm, its address, the interrogation messages, the frequency at which these messages are dispatched, the limit time between two messages before switching, as well as other configuration parameters are notably installed in a configuration file contained in each router. Several types of these parameters can be stored in this configuration file, each type depending on the type of end application. On initializing the routers, the parameters specific to an application are for example offloaded to a random access memory. The management of the various software layers, including the reset to zero algorithm, as well as the communications between these layers are processed conventionally by an operating system, possibly associated with intermediate software layers, called "middleware" in the literature, installed in the routers.

The invention has been described in respect of a computerized routing device, a router being associated with a redundant router. The invention can of course be applied to other input/output management means, such as for example data servers. It is advantageously applied to all types of applications requiring high security of operation with economy requirements. Additionally, it

is simple to implement, since this implementation is essentially software based.

Claims

1. Device for digital data input and output management, characterized in that it comprises first management means (1) and second management means (2) connected together by two interfaces, a network (23) and a security line (24), these means mutually exchanging interrogation messages through these two interfaces (23,24), means (1) being considered to be faulty by the other means (2) when they do not send any message in a given time interval on at least one of the two interfaces (23,24).

2. Device according to Claim 1, characterized in that when operation thereof is initialized, the first means (1) have the role of master and the second means (2) have the role of slave, the master managing the input and output data.

3. Device according to any one of the preceding claims, characterized in that the means (1,2) are connected by the network (23) to one or more systems (21,22).

4. Device according to any one of the preceding claims, characterized in that they are connected by one or more series links to systems, a y-type cable (5) connecting one and the same port (3) of each router to a system.

5. Device according to any one of the preceding claims, characterized in that the means (1,2) have the same functions and comprise the same software and same configuration files.

6. Device according to any one of the preceding claims, characterized in that when means (1) are

detected as being faulty by the other means (2), the latter deactivate the faulty means.

7. Device according to Claims 2 and 6, characterized in that the defective means (1) being the master, the slave deactivates the inputs/outputs of the master and activates its own inputs/outputs.

8. Device according to any one of the preceding claims, characterized in that it comprises at least one algorithm for resetting the first and second means (1,2) to zero, the faulty means (1) being deactivated and the other means (2) activated upon reinitialization after detection of a fault.

9. Device according to any one of the preceding claims, characterized in that the interrogation messages, the frequency at which these messages are dispatched, the limit time between two messages are installed in a configuration file contained in each of the means (1,2), several types of these parameters being stored depending on given applications.

10. Device according to Claim 9, characterized in that when the means (1,2) are initialized, the parameters specific to an application are offloaded to a random access memory.

11. Device according to any one of the preceding claims, characterized in that it comprises alert means for forewarning of a fault.

12. Device according to any one of the preceding claims, characterized in that the network is a local area digital network.

13. Device according to any one of the preceding claims, characterized in that the input/output data management means are computer routers.

14. Device according to Claim 13, characterized in that the routers operate in OCP open mode.

15. Device according to any one of Claims 1 to 12, characterized in that the input/output data management means are data servers.

Abstract

Redundant input/output management device, notably for computerized routing

The present invention relates to a redundant input/output management device, notably a computerized routing system.

The device comprises first management means (1) and second management means (2) connected together by two interfaces, a network (23) and a security line (24), these means mutually exchanging interrogation messages through these two interfaces (23,24), means (1) being considered to be faulty by the other means (2) when they do not send any message in a given time interval on at least one of the two interfaces (23,24).

The invention applies in particular in respect of the processing of air traffic management information. More generally, it applies in respect of all digital data input and output management systems requiring high security of operation without excessive cost overheads.

Figure 2

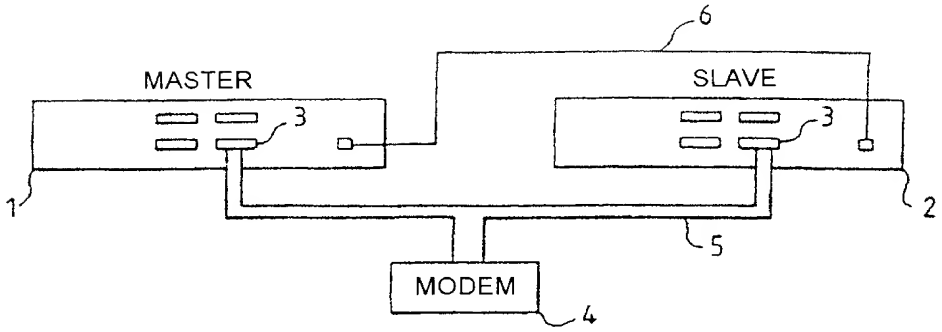
6
MASTER
SLAVE
3
3
1
2
5
MODEM
4

FIG.1

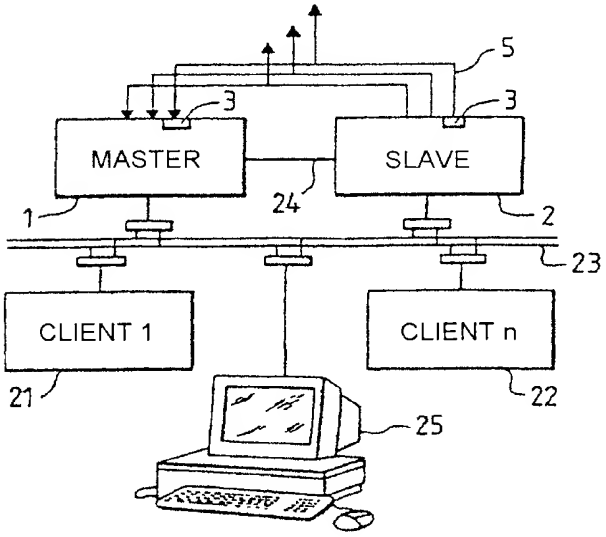
5
3
3
MASTER
SLAVE
24
1
2
23
CLIENT 1
CLIENT n
21
22
25

FIG.2

Abstract